CLAIMS

What is claimed is:

1. A method comprising:

providing a key matrix having N rows and M columns of matrix keys, where N≥2 and M≥2;

for each column of the key matrix, performing arithmetic operations on matrix keys of at least two selected rows of the key matrix to produce a first set of secret device keys;

producing a shared secret key based on arithmetic operations on selected secret device keys of the first set of secret device keys.

2. The method of claim 1, wherein the arithmetic operations include modular addition.

3. The method of claim 1, wherein prior to performing the arithmetic operations, the method comprises:

generating a key selection vector identifying the at least two selected rows of the key matrix from which to produce the first set of secret device keys.

4. The method of claim 3, wherein the key selection vector is uniquely assigned to a first digital platform.

5. The method of claim 4, wherein prior to producing the shared secret key, the method comprises:

receiving a key selection vector from a second digital platform in communication with the first digital platform; and

analyzing contents of the key selection vector from the second digital platform to determine the selected secret device keys of the first set of secret device keys.

6. The method of claim 1, wherein prior to performing arithmetic operations on keys of at least two selected rows, the method further comprises:

dedicating the rows of the key matrix to a first classification; and

dedicating the columns of the key matrix to a second classification.

7. The method of claim 6, wherein the first classification includes digital platforms designed to provide information to other digital platforms.

8. The method of claim 7, wherein the second classification includes digital platforms designed to receive information from other digital platforms.

9. The method of claim 1, wherein the producing of the shared secret key comprises:

analyzing contents of an incoming key selection vector; and

performing arithmetic operations of the selected secret device keys located in columns of the key matrix identified by the contents of the incoming key selection vector.

10. The method of claim 9, wherein the producing of the shared secret key further comprises:

performing a hash operation on results of the arithmetic operations of the selected secret device keys located in the column of the key matrix identified by the contents of the incoming key selection vector.

11. A method comprising:

providing a key matrix having N rows and M columns of matrix keys, where N≥2 and M≥2;

for each row of the key matrix, performing arithmetic operations on matrix keys of at least two selected columns of the key matrix to produce a first set of secret device keys;

producing a shared secret key based on arithmetic operations on selected secret device keys of the first set of secret device keys.

12. The method of claim 11, wherein the arithmetic operations include modular addition.

13. The method of claim 11, wherein prior to performing the arithmetic operations, the method comprises:

generating a key selection vector identifying the at least two selected rows of the key matrix from which to produce the first set of secret device keys.

14. The method of claim 13, wherein the key selection vector is uniquely assigned to a first digital platform.

15. The method of claim 14, wherein prior to producing the shared secret key, the method comprises:

receiving a key selection vector from a second digital platform in communication with the first digital platform; and

analyzing contents of the key selection vector from the second digital platform to determine the selected secret device keys of the first set of secret device keys.

16. The method of claim 1, wherein prior to performing arithmetic operations on keys of at least two selected columns, the method further comprises:

dedicating the rows of the key matrix to a first classification; and

dedicating the columns of the key matrix to a second classification.

17. The method of claim 11, wherein the producing of the shared secret key comprises:

analyzing contents of an incoming key selection vector; and

performing arithmetic operations of the selected secret device keys located in rows of the key matrix identified by the contents of the incoming key selection vector.

18. The method of claim 17, wherein the producing of the shared secret key further comprises:

performing a hash operation on results of the arithmetic operations of the selected secret device keys located in the rows of the key matrix identified by the contents of the incoming key selection vector.

19. A machine readable medium having embodied thereon a computer program for processing by a first digital platform including memory containing the computer program comprising:

an authentication function to recover an incoming key selection vector and to compute a shared secret key based on a set of secret device keys stored in the first digital platform and the contents of the incoming key selection vector;

a transfer function to output at least a key selection vector assigned to the first digital platform;

a hash function to perform a hash operation on at least the shared secret key to produce a resultant hash value; and

a comparison function to compare the resultant hash value with an incoming check hash value received subsequent to the transmission of the key selection vector.

20. A network comprising:

a first digital platform; and

a certification authority in communication with the first digital platform, the certification authority having access to a key matrix featuring matrix keys arranged in accordance with at least a first dimension and a second dimension, generating a first key selection vector and providing a first set of secret device keys produced from selected matrix keys of the key matrix.

21. The network of claim 20 further comprising:

a second digital platform in communication with the certification authority and the first digital platform, the second digital platform being uniquely assigned a second key selection vector indicating at least two grids of the key matrix and a second set of secret device keys produced from matrix keys situated in at least two grids of the key matrix.

22. The network of claim 21, wherein the first and second digital platforms to exchange the first and second key selection vectors in order for each digital platform to produce a shared secret key to ensure that communications between the first and second digital platforms are secure.

23. A certification authority comprising:

a memory to store a key matrix having N rows and M columns of matrix keys, where $N \geq 2$ and $M \geq 2$;

a logic to generate a key selection vector for each digital platform registered with the certification authority.

24. The certification authority of claim 23, wherein the logic includes a processing unit.

25. The certification authority of claim 24, wherein the processing unit produces a first set of secret device keys by performing arithmetic operations on matrix keys along selected columns of the key matrix identified by the key selection vector to provide a first set of secret device keys to a digital platform.

26. The certification authority of claim 25, wherein the matrix keys along the processing unit performs arithmetic operations on matrix keys along selected rows of the key matrix identified by the key selection vector to provide a first set of secret device keys to a digital platform.

27. The certification authority of claim 23, wherein the matrix keys are only known by the certification authority.